This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (original): A method of testing a network firewall, comprising:

transmitting a communications session initiation signal from said signal source using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall;

transmitting test signals from said signal source, following initiation of said communications session and prior to termination of said initiated communications session, at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address;

monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall; and

identifying any open ports that are not associated with said established communications session, which passed at least one of said transmitted test signals, as erroneously open ports.

2. (original): The method of claim 1, wherein said transmitted test signals are IP packets which include said IP address as a source address.

3. (original): The method of claim 1, further comprising:

determining from at least one session initiation signal at least one port associated with the established communication session that should be open; and

generating an error signal indicating that said at least one port associated with the established communication session is erroneously closed if a test signal is not detected passing through said port to the second side of said firewall.

4. (original): The method of claim 3, further comprising, prior to transmitting said communications session initiation signal,

transmitting a first test signal at the first side of said network firewall from the signal source using an IP address that is not associated with any ongoing communications session being conducted through said firewall;

monitoring the second side of said firewall to determine if said first test signal passed through said firewall; and

reporting a firewall error if it is determined that said first signal passed through said firewall.

5. (original): The method of claim 3, wherein said transmitting steps are performed by a first test device and said monitoring steps are performed by a second test device, the second test device being physically separate from said first test device, the method further comprising:

synchronizing the first and second test devices to a common clock located external to said first and second test devices.

6. (original): The method of claim 5, further comprising;

operating the first test device to communicate information identifying ports through which test signals were detected passing through said firewall from the second side to the second test device; and

operating the second test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side.

7. (original): The method of claim 5, further comprising;

operating the second test device to communicate information identifying ports through which test signals were detected passing through said firewall from the first side to the first test device; and

operating the first test device to generate a test report including information about the status of unidirectional ports used to communicate signals from the first side to the second side and unidirectional ports used to communicate signals from the second side to the first side.

8. (original): The method of claim 7, wherein said session signal is at least one of SIP

and H.323 compliant signals.

9. (currently amended): A firewall test system, comprising:

a first test device located on an untrusted side of said firewall, the first test device including:

i) a session signal generator for transmitting a communications session initiation signal using an IP address corresponding to said signal source to establish a communications session to be conducted through said firewall;

ii) a probe signal generator for generating test signals at a range of ports in a first side of said firewall through which media signals may be transmitted when said ports are open, said test signals including said IP address; and

iii) timing synchronization circuitry for synchronizing said session signal generator and said probe signal generator to at least one of another test device and a clock signal source located external to said first test device; and

a second test device located on ~~an~~ a trusted side of said firewall, the ~~first~~ second test device including:

means for monitoring a second side of said firewall to detect any transmitted test signals that pass through said firewall; and

an analysis module for identifying any open ports that are not associated with an established communications session, which passed at least one of said transmitted test signals, as erroneously open ports.

10. (original): The system of claim 9, wherein said probe signal generator generates IP packets which include said IP address as a source address.

11. (original): The system of claim 9, wherein said analysis module includes:

means for determining from at least one session initiation signal at least one port associated with the established communication session that should be open; and

means for generating an error signal indicating that said at least one port

associated with the established communication session is erroneously closed if a test signal is not detected passing through said port to the second side of said firewall.

12. (original): The system of claim 11, wherein the test signal generator of said first test device includes:

means for transmitting a first test signal at the first side of said network firewall from the signal source using an IP address that is not associated with any ongoing communications session being conducted through said firewall prior to said communications session initiation signal being generated.

13. (original): The system of claim 11, wherein said first test device further includes:

an analysis module for monitoring the second side of said firewall to determine if said first test signal passed through said firewall; and

a report generation module for reporting a firewall error if it is determined that said first signal passed through said firewall.

14. (original): The system of claim 9, wherein said session signal generates at least one of SIP and H.323 compliant signals.